# Cyberrisico's verminderen

**Vanaf 25 mei 2018 kunnen bedrijven en organisaties worden aangesproken op het naleven van de Algemene Verordening Gegevensbescherming (AVG). Dit houdt onder andere in dat aangetoond moet kunnen worden hoe persoonsgegevens worden verwerkt en dat datalekken verplicht binnen 72 uur moeten worden gemeld. Bedrijven en organisaties die hierin falen, riskeren boetes die kunnen oplopen tot 20 miljoen euro of 4 procent van de jaarlijkse wereldwijde omzet. Risicoadviseur en verzekeringsmakelaar Aon helpt bedrijven en organisaties succesvol te ondernemen met een stappenplan om tijdig te voldoen aan de AVG en het afstemmen van verzekeringen op de toenemende cyberrisico's in de huidige digitale wereld.**

Nog niet eens zo heel lang geleden hielden security managers zich voornamelijk bezig met de fysieke beveiliging van gebouwen, goederen en mensen. Dit gebeurde onder meer door middel van inbraak- en branddetectie, toegangscontrole, terreinbeveiliging en aanvullend cameratoezicht. Veelal betroffen dit separate systemen van verschillende leveranciers waarvoor per systeem onderhoudscontracten waren afgesloten. De beveiliging van elektronische data zoals klantgegevens en salarisadministratie was de verantwoordelijkheid van de IT-afdeling. Deze hield het netwerkverkeer in de gaten, installeerde antivirussoftware en updates op de bedrijfscomputers en servers en onderstreepte het belang van sterke wachtwoorden en bewust internetgedrag naar medewerkers. Natuurlijk was er regelmatig overleg tussen beide afdelingen, maar in de praktijk waren het veelal gescheiden werelden. De IT-afdeling bemoeide zich niet met de individuele toegangsrechten per werknemer of de posities van camera's en de security manager hield zich niet bezig met hoe de toegangsrechten en camerabeelden werden opgeslagen. Zo lang de beschikbaarheid van deze data maar was gegarandeerd, was het niet aan de security manager om te bepalen of deze bijvoorbeeld moest worden versleuteld.

**Downtime** De scheidslijnen tussen deze werelden met ieder hun eigen expertises en organisatiestructuur zijn echter steeds meer aan het vervagen. Beveiligingssystemen communiceren via het netwerk en zijn te bedienen en beheren met dezelfde gebruikersinterface of via een app op afstand met smartphones of tablets. De fysieke beveiliging van gebouwen is onverminderd belangrijk gebleven, maar het accent ligt op de continuïteit van processen en het beveiligen van gevoelige bedrijfsgegevens. De 'kroonjuwelen' van bedrijven en organisaties zijn overwegend digitaal en niet te beveiligen met deuren, slagbomen of hekwerken. De risicoprofielen zijn aanzienlijk veranderd en de uitdagingen waarmee security managers dagelijks hebben te maken zijn veelzijdiger en complexer dan ooit. Bedrijven en organisaties worden geconfronteerd met uiteenlopende cyberdreigingen die tot het verlies van data of verstoring van bedrijfsprocessen kunnen leiden. Criminelen die het hebben gemunt op bedrijfsdata hoeven niet zelf aanwezig te zijn in bedrijfspanden om toegang te krijgen tot databases en ook de eigen medewerkers kunnen voor gevaar zorgen door gegevens naar persoonlijke mailadressen te sturen of te kopiëren op een USB-stick. De schadepost is aanzienlijk als het netwerk gedurende langere tijd onbereikbaar is. Een 'downtime' van enkele uren betekent dat het leeuwendeel van de medewerkers hun taken niet kunnen uitvoeren en klanten geen bestellingen kunnen plaatsen. De verschillende afdelingen die verantwoordelijk zijn voor de bedrijfscontinuïteit moeten meer dan ooit met elkaar communiceren om gezamenlijk de risico's te definiëren en een adequate aanpak af te stemmen om de gevolgen zoveel mogelijk te beperken.

**Materiële schade** Na een aanval door hackers waarbij gegevens zijn gestolen of het netwerk gedurende een lange periode uit de lucht is geweest, heeft het zo snel mogelijk volledig kunnen hervatten van de bedrijfsprocessen de hoogste prioriteit. Daarna is het zaak het incident te analyseren om lessen voor de toekomst te kunnen trekken, de geleden schade in kaart te brengen en bepalen of en hoe deze valt te verhalen. Dat laatste blijkt bij hackers over het algemeen uiterst moeilijk, zelfs als ze worden aangehouden en veroordeeld. Uit onderzoeken naar bedrijfscontinuïteit blijkt dat bedrijven het vaak lastig vinden de door downtime geleden schade te kwantificeren. Het aantal uren waarin werknemers en uitzendkrachten buiten hun schuld niet productief zijn geweest is aantoonbaar te maken, maar het aantal misgelopen orders is minder eenvoudig te calculeren. En dan is er nog de imagoschade: klanten kijken bijvoorbeeld de kat uit de boom en stellen nieuwe bestellingen uit omdat zij twijfelen of de bestelde goederen daadwerkelijk zullen worden geleverd en of hun (privé)data wel veilig is bij deze organisatie. Hoeveel bedraagt die schade en welk deel daarvan wordt gedekt door de verzekeringen? "Bedrijven en organisaties doen er goed aan hun bestaande verzekeringen tegen het licht te houden. Zeker verzekeringen die

# en verzekeren


al geruime tijd geleden zijn afgesloten, bieden geen dekking tegen allerlei cyberrisico's", vertelt Sjaak Schouteren, Manager Cyber Risk Solutions bij Aon Risk Solutions. "Aansprakelijkheidverzekeringen treden in werking bij zaak- of letselschade. Een property verzekering als er sprake is van materiële schade. Hier is in het geval van een cyberincident vaak geen sprake van. Hierdoor is er ook geen dekking voor de gevolgschade op de reguliere polissen. Dit terwijl de schade als gevolg van grote branden per jaar 600 miljoen euro is. De kosten als gevolg van cyberincidenten is in Nederland 10 miljard euro."

**Datalekken** Bedrijven en organisaties lijken zich niet altijd te realiseren dat lang niet alle schade door onder meer datalekken, virussen of ransomware zoals het recente WannaCry wordt gedekt. "Dat komt ook doordat wij als verzekeringsmarkt de afgelopen jaren niet altijd even duidelijk zijn geweest op dit gebied", zegt Schouteren. "Bedrijven dienen zich te realiseren dat Cyber Risk Management meer is dan alleen het treffen van technische voorzorgsmaatregelen op het gebied van IT en dat een verzekering een onderdeel is van een heel traject. Belangrijk is ook om te kijken wat men aan de voorkant kan voorkomen, waarbij het vergroten van het bewustzijn van medewerkers erg belangrijk is."
Vanaf 25 mei volgend jaar is er nog een extra stok achter de deur om de bestaande verzekeringen af te stemmen op het veranderende risico. Vanaf die datum moeten bedrijven kunnen aantonen te voldoen aan de Algemene Verordening Gegevensbescherming. De AVG, ook bekend als General Data Protection Regulation (GDPR), trad op 24 mei 2016 in werking als vervanger van de uit 1995 daterende databeschermingsrichtlijn die niet meer aansloot op de hedendaagse digitale wereld. Van bedrijven en organisaties wordt verwacht dat zij hun bedrijfsvoering met de AVG in overeenstemming brengen. Zo moeten zij aantonen hoe persoonsgegevens worden verwerkt, dat gegevens niet langer worden bewaard dan wettelijk is toegestaan en dienen datalekken verplicht binnen 72 uur te worden gemeld. Bedrijven kunnen hierop worden aangesproken door iedereen waarvan gegevens zijn vastgelegd, van klanten en leveranciers tot eigen personeel. Meldingen van het niet naleven van de AVG worden onderzocht door de Autoriteit Persoonsgegevens (AP), die boetes kan opleggen tot 20 miljoen euro of 4 procent van de jaarlijkse wereldwijde omzet. Opsporingsinstanties en het Openbaar Ministerie zijn vrijgesteld van de AVG, omdat zij onder aparte privacywetgeving vallen.
Naast de dekking voor de gederfde netto winst in verband met netwerkonderbreking biedt een cyberverzekering onder andere ook dekking van de boetes van de AP. Maar belangrijker nog ondersteunt de organisatie door middel van een panel van experts (advocaten, forensisch experts en communicatie/PR experts) om de schade die is ontstaan door bijvoorbeeld een datalek te minimaliseren en dekt ook de aanspraken van derden als gevolg van een datalek.

**Drijfveer** Dat Nederlandse bedrijven met datalekken te maken hebben, blijkt onder meer uit recente cijfers van de AP. In het eerste kwartaal van 2017 werden 2300 datalekken bij deze instantie gemeld, met name vanuit de sectoren gezondheid en welzijn, financiële dienstverlening en openbaar bestuur. In deze periode werden 135 onderzoeken gestart naar beveiliging en (mogelijke) datalekken, ook bij organisaties die deze niet zelf hadden gemeld. Het merendeel van de onderzochte organisaties kreeg een waarschuwing, maar boetes werden niet uitgedeeld. In 2016, het eerste jaar waarin datalekken moesten worden gemeld, werden 5693 meldingen gedaan. Voorbeelden waren het kwijtraken van USB-sticks met privacygevoelige gegevens, poststukken die geopend retour kwamen en klanten die gegevens van andere personen konden inzien.
Sjaak Schouteren: "De stijging van het aantal meldingen is mede te verklaren door het toegenomen bewustzijn binnen organisaties. Als een mail met bepaalde gegevens per ongeluk naar een verkeerde persoon wordt verstuurd, nemen bedrijven tegenwoordig het zekere voor het onzekere en melden dit." Toch hoeven bedrijven niet direct te vrezen voor de torenhoge boetes. Schouteren: "De kans dat een boete van 20 miljoen euro wordt uitgedeeld in Nederland is niet groot. De boetes moeten ook niet de drijfveer zijn om compliant te zijn met de AVG. Door onder meer te laten zien dat gevoelige gegevens veilig worden beheerd en verwerkt tonen bedrijven aan dat zij er alles aan hebben gedaan om cyberincidenten te voorkomen. Dat kan worden benadrukt als Unique Selling Point." ▸

**Stappenplan** Volgens Schouteren is het ondoenlijk om honderd procent te voldoen aan de AVG. "De verordening is er natuurlijk niet voor niets gekomen, maar volledig compliant zijn betekent dat ondernemers bijna geen zaken meer kunnen doen. Onze experts hebben de AVG in zijn geheel geanalyseerd en gerubriceerd. Met klanten kijken we via een nulmeting waar zij staan ten opzichte van de AVG. Zijn er verwerkingsovereenkomsten opgesteld en Privacy Impact Analyses (PIA) uitgevoerd? Bij het uitvoeren van een PIA kijken wij zeer pragmatisch naar welke risico's we hoe kunnen verminderen. Hierbij moeten we beseffen dat je elke euro maar één keer kunt uitgeven. Door middel van een PIA maken wij samen met de stakeholders inzichtelijk welke risico's er zijn, wat de klant zelf kan doen om de risico's te beperken en waarin ze nog moeten investeren. Bedrijven kiezen er soms bijvoorbeeld uit kostenoverwegingen bewust voor om niet iedere computer in de organisatie te willen voorzien van encryptie. Middels een PIA kan dan worden besloten welke computers wel encryptie krijgen en welke niet. Op die manier is naar klanten en leveranciers en ook naar de AP direct aan te geven welke maatregelen zijn ondernomen en waarom. Waar het accent ligt en welke 'restrisico's' overblijven, verschilt voor ieder bedrijf."

Om bedrijven en organisaties te helpen te voldoen aan de AVG, heeft Aon een stappenplan opgesteld.

**• Veranker privacy- en gegevensbescherming op het hoogste niveau binnen de organisatie.**

Schouteren: "In de praktijk blijkt dat er veel afdelingen bij het proces zijn betrokken: IT, Security, HRM, Marketing & Communicatie, Legal. Maar zonder de steun van de directie is het lastig om privacybescherming binnen de organisatie door te voeren."

**• Voer een analyse uit om privacyrisico's te identificeren en middels passende technische en organisatorische maatregelen te beheersen (PIA).**

Een groot privacyrisico is bijvoorbeeld het niet goed instellen van gebruikersrechten waardoor meer werknemers en medewerkers van externe dienstverleners bij privacygevoelige data kunnen dan voor het uitvoeren van hun dagelijkse werkzaamheden noodzakelijk is.

**• Maak een verwerkingsregister waarin wordt vastgelegd hoe privacygevoelige gegevens worden verwerkt.**

Dit is al verplicht onder de Wet bescherming persoonsgegevens (Wbp), dus bedrijven horen momenteel een dergelijk verwerkingsregister al op orde te hebben. De praktijk leert echter dat dit of niet is gebeurd of nooit meer up-to-date is gebracht.

**• Classificeer persoonsgegevens zodanig dat wordt voldaan aan wettelijke bewaartermijnen en gegevens tijdig kunnen worden verwijderd.**

Schouteren: "Bij bedrijven blijkt vaak dat er veel meer gegevens van voormalige dan van bestaande klanten in de database staan. Dat gebeurt dan omdat het arbeidsintensief zou zijn om alle gegevens te verwijderen. Maar voormalige klanten hebben het recht om hun gegevens te kunnen inzien en te laten verwijderen. Minimaliseer data door op voorhand al niet om gegevens te vragen die niet strikt noodzakelijk zijn. Let er daarbij ook op dat data zowel intern als extern kan zijn opgeslagen."

**• Evalueer bestaande contracten met partijen waarmee gegevens worden gedeeld.**

Let hierbij ook op het inschakelen van derden en onderaannemers en wat de locatie is waar de data wordt verwerkt.

**• Stel een procedure op voor het adequaat anticiperen en afhandelen van een datalek.**

**Sjaak Schouteren, Manager Cyber Risk Solutions bij Aon Risk Solutions.**

Schouteren: "Een datalek moet binnen 72 uur worden gemeld. Houd daarmee rekening bij het outsourcen van bijvoorbeeld de salarisadministratie. Het bedrijf blijft zelf verantwoordelijk voor die data. Als in een meerjarige SLA staat dat de dienstverlener (verwerker) binnen acht kantooruren melding moet maken van een datalek aan de verantwoordelijke en er een datalek wordt geconstateerd op vrijdag 10.00 uur, dan zou een melding naar de verantwoordelijke organisatie op maandagochtend om 10.00 uur ook voldoende zijn. Dit geeft de verantwoordelijke organisatie echter geen tijd meer om het lek adequaat te melden bij de Autoriteit Persoonsgegevens."

**• Verhoog het privacybewustzijn van medewerkers door gerichte activiteiten.**

De medewerkers verwerken de meeste data en hebben daar toegang toe. Weten zij wel wat een datalek is en hoe ze moeten omgaan met data?

**• Stel privacybeleid op gebaseerd op de AVG of pas het bestaande beleid hierop aan.**

In privacystatements wordt vaak vermeld dat een organisatie voldoet aan de regelgeving, terwijl uit onderzoek blijkt dat dit vaak niet het geval is. Hierdoor wek je de valse verwachting van veiligheid en compliance met alle gevolgen van dien mocht het fout gaan.

**• Informeer de betrokkenen over wat er met hun persoonsgegevens gebeurt.**

Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Bedrijven en organisaties riskeren een boete als zij de rechten van de betrokkenen niet naleven.

**• Stel vast of de organisatie over een functionaris gegevensbescherming moet beschikken.**

Een dergelijke functionaris is in veel gevallen verplicht. Deze moet dan ook worden aangesteld en de juiste taken krijgen toebedeeld. Bijvoorbeeld in de zorgsector is deze functionaris al vanaf 1 juli 2017 verplicht.

■ Robert van Daesdonk
Redactie@beveiliging.nl

**Meer informatie is te vinden op www.aon.nl/cyber**